UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/557,750	10/30/2006	Pekka Nikander	3772-27	2289

23117 7590 06/05/2009

NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

EXAMINER	
THAO, CHHEAN K	
ART UNIT	PAPER NUMBER
2617	

MAIL DATE	DELIVERY MODE
06/05/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/557,750	NIKANDER ET AL.	
	Examiner	Art Unit	
	CHHEAN THAO	2617	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *March 18,2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22 are cancelled; 23-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22 are cancelled; 23-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Detail Office Action

1. Claims 1-22 (cancelled); claims 23-30 are added.

2. **Response to Arguments**

Applicant's arguments with respect to claim 23-30 have been considered but are moot based on new added claims rejection.

Applicant's arguments with respect to claim 23-30 have been considered but are moot in view of the new ground(s) of rejection.

Applicant's arguments filed March 18, 2009 have been fully considered but they are not persuasive.

Regarding the response filed, applicant argues that "Haverinen does not disclose re-running an authentication and key agreement procedure to achieve this functionality. Nor does Haverinen teach assigning an FQDN and/or IP address to the mobile node by making use the subscriber contact information collected by the stable forwarding agent from the authentication server". Although, examiner agrees with applicant that Haverinen may not specifically discloses the term "re-running"; however, **column 12 lines 5-56, "the MT sends to the FAAA a Network Access Identifier NAI and a protection code MT_RAND (also known in Mobile IP terminology as nonce) generated by the MT; the FAAA sends to the HAAA an initial identification message containing the IMSI or NAI of the MT, and the MT_RAND.; the HAAA retrieves n GSM triplets, each comprising a RAND, a Kc, and a SRES. Then, the HAAA computes the K=H(n*Kc,MT_RAND) for the MT". In addition, figure 2 clearly depicts the re-run authentication procedure to ensure data security. Weschler, column 16 lines 1-12, teaches " re-running the hashing function". Finally, Haverinen, column 1 lines 27-51, "A mobile node belongs to a home network to which belongs a home agent of the**

mobile node. The HA is a router on a mobile node's home network which tunnels datagrams for delivery to the mobile node when it is away from home, and maintains current location information for the mobile node. A mobile node is given a long-term IP address". Haverinen, column 2 lines 35-37, discloses "**the IP network's terminal (TE1) uses a subscriber identity module**". Thus, based on new ground of rejection, the combination of Haverinen and Weschler teach all of the limitations in the claimed invention. Therefore, applicant's argument is non-persuasive.

3. Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 23-30 are rejected under 35 U.SC. 103(a) as being unpatentable over Haverinen (US 7107620 B2) in view of Weschler (US 6807181 B1).

Regarding claim 23, Haverinen discloses a method of securely initializing subscriber and security data in a mobile routing system when the subscribers are also subscribers of a radio communication network, the method comprising:

re-running an authentication and key agreement procedure defined for the radio communication

network, between a mobile node and an authentication server of the radio communication network (**The MT sends to the FAAA a Network Access Identifier NAI and a protection code MT_RAND (also known in Mobile IP terminology as nonce) generated by the MT; the FAAA sends to the HAAA an initial identification message containing the IMSI or NAI of the MT, and the MT_RAND. ; the HAAA retrieves n GSM triplets, each com prising a RAND, a Kc, and a SRES. Then, the HAAA computes the K=H(n*Kc,MT_RAND) for the MT; figure 2 clearly depicts the re-run authentication procedure to ensure security; therefore, re-running and authentication and key agreement procedure; see column 12 lines 5-56);**

providing a shared secret resulting from the re-running of the authentication and key agreement procedure to a stable forwarding agent of the mobile routing system, and using the shared secret to authenticate the mobile node to the stable forwarding agent (**a shared session key K is generated both in the MT and in the FAAA server; Haverinen, column 11 lines 54-67 and column 12 lines 1-56**);

agreeing upon keys by which further communications between the mobile node and the stable forwarding agent can be secured (**In the MT, the calculation of the K is the same as the calculation of the K in the HAAA; if the SIGNsres is valid, the HAAA sends also the K to the FAAA; Authentication is complete and the FAAA and the MT share the K; see Column 12 lines 45-56);**

following authentication of the mobile node to the stable forwarding agent, collecting at the stable forwarding agent subscriber contact information from said authentication server (**utilising the secret shared between the telecommunications network and the mobile node, subscriber**

identity modules (a subscriber identity for identifying the subscriber) can be used for strong mutual authentication; see column 8 lines 50-55); and

using the subscriber information and keys in providing mobility services to subscriber mobile nodes and correspondent nodes, including using the subscriber information to assign a Fully Qualified Domain Name and/or IP address to the mobile node (**the PAC allocates an IP address to the MT and authenticates the MT before connection to the Internet is established. The PAC relays the authentication messages between the MT and the GAGW, collects the billing record and sends it to GAGW. The PAC also relays user data traffic between the MT and the Internet; see column 20 lines 44-49).**

Although the authentication processes describes in column 12 and figure 2 by Haverinen show a "re-running" of authentication and key agreement procedure, Haverinen fails to specifically teach the term "re-run"

However, the preceding limitation is known in the art of communication. The second reference, Weschler teaches re-running authentication and key agreement process **(the certification methods 622 allow the sender to digitally "sign" the control data, thereby authenticating its origin and content, and increasing the security of the client/server communication. Basically, signing a message is a two step process, run through a hashing algorithm and re-running the hashing function; Weschler, column 16 lines 1-12).** Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to implement the technique of Weschler within the system of Haverinen in order to create a secure data transfer through a re-authentication and key agreement process.

Regarding claim 24, the combination of Haverinen and Weschler disclose a method according to claim 23, further comprising:

transporting messages associated with the re-running step, between the stable forwarding agent used by a mobile node and the authentication server via the stable forwarding agent (**In the MT (MT belongs to HA, and HA (stable forwarding agent) is a router on an MT), the calculation of the K is the same as the calculation of the K in the HAAA; if the SIGNsres is valid, the HAAA sends also the K to the FAAA; Authentication is complete and the FAAA and the MT share the K; see Column 12 lines 45-56).**

Regarding claim 25, the combination of Haverinen and Weschler disclose a method according to claim 23, further comprising:

sending session keys, agreed upon during the re-run authentication procedure, from the authentication server to the stable forwarding agent (**The FAAA sends the SIGNsres to the HAAA, SIGNsres=HASH2(K,n*SRES) for the K and the SRESs; see Column 12 lines 7-48).**

Regarding claim 26, the combination of Haverinen and Weschler disclose a method according to claim 23, further wherein the mobile routing system is a Mobile IP based system, and the stable forwarding agent is a Home Agent (**Home Agent (HA), column 1 line 27; mobile IP network; column 4 line 19).**

Regarding claim 27, the combination of Haverinen and Weschler disclose a method according to claim 23, wherein the mobile routing system is a HIP based system (**column 28 lines 55-60, where Haverinen discuss public key technique, therefore HIP based system; Gateway (i.e., router, therefore a Forwarding Agent), Column 5, line 44)**.

Regarding claim 28, the combination of Haverinen and Weschler disclose a method according to claim 23, wherein said authentication and key agreement procedure is the Authentication and Key Agreement procedure specified by 3GPP (**the Subscriber Identity Module is used in generating of the session secret based on a shared secret specific for the mobile node identity, column 3 lines 54-58; retrieving from the subscriber identity module to the mobile node the mobile node identity and a session secret specific to the mobile node identity, column 4 line 46-48**; **therefore, 3GPP procedure**).

Regarding claim 29, the combination of Haverinen and Weschler disclose a method according to claim 23, wherein the collected subscriber information comprises one or more of the following:

the name and postal address of a subscriber **(the home GSM network stores customer information, such as authentication codes and user identity; therefore, name and postal address of subscriber; column 19 lines 60-63)**

the telephone number associated with a subscriber (**the home GSM network stores customer information, such as authentication codes and user identity; therefore, telephone number of subscriber; column 19 lines 60-63**);

the existing Fully Qualified Domain Name for a subscriber **(The NAI is in form of imsi@sonera.fi (for example "1234567@sonera.fi") or imsi@gsm.org (for example "1234567@gsm.org"); column 10 lines 15-24**); and the status of any mobility services established earlier for a subscriber (**the MT needs first to send its IMSI to the MA with which it is registering. Then the MA is able to use the FAAA-HAAA protocol in order to obtain**

GSM authentication information for the MT (as described above) and use this information for generating the K, with the MT;column 14 lines 25-34).

Regarding claim 30, Haverinen discloses a stable forwarding agent of a mobile routing system, the stable forwarding agent comprising:

a relay for relaying messages associated with a re-run of an authentication and key agreement procedure between a mobile node and an authentication node of a radio communication network (**The MT sends to the FAAA a Network Access Identifier NAI and a protection code MT_RAND (also known in Mobile IP terminology as nonce) generated by the MT; the FAAA sends to the HAAA an initial identification message containing the IMSI or NAI of the MT, and the MT_RAND. ; the HAAA retrieves n GSM triplets, each com prising a RAND, a Kc, and a SRES. Then, the HAAA computes the K=H(n*Kc,MT_RAND) for the MT; figure 2 clearly depicts the re-run authentication procedure to ensure security; therefore, re-running and authentication and key agreement procedure; see column 12 lines 5-56)**;

a receiver for receiving a shared secret from the authentication server following completion of the procedure for using the shared secret to authenticate the mobile node and for collecting subscriber contact information from the authentication server (**utilising the secret shared between the telecommunications network and the mobile node, subscriber identity modules (a subscriber identity for identifying the subscriber) can be used for strong mutual authentication; see column 8 lines 50-55**);

a key determining processor for agreeing upon keys by which further communications between the mobile node and the stable forwarding agent can be secured (**The MT detects that SIM**

authentication is supported. The ME requests the IMSI from the SIM_B. 304. The SIM_B responds to the IMSI request 303 by sending the IMSI to the ME; a secure channel is formed between the PAC and the GAGW using their previously; column 21 lines 25-44); and

a mobility service provisioning processor for using said subscriber information and keys in the provision of mobility services to subscriber mobile nodes including using the subscriber information to assign a suitable Fully Qualified Domain Name and/or IP address to said mobile node (**the PAC allocates an IP address to the MT and authenticates the MT before connection to the Internet is established. The PAC relays the authentication messages between the MT and the GAGW, collects the billing record and sends it to GAGW. The PAC also relays user data traffic between the MT and the Internet; see column 20 lines 44-49; a mobile node is given a long-term IP address, column 1 lines 42-67).**

Although the authentication processes describes in column 12 and figure 2 by Haverinen show a "re-run" of authentication and key agreement procedure, Haverinen fails to specifically teach the term "re-run"

However, the preceding limitation is known in the art of communication. The second reference, Weschler teaches re-running authentication and key agreement process **(the certification methods 622 allow the sender to digitally "sign" the control data, thereby authenticating its origin and content, and increasing the security of the client/server communication. Basically, signing a message is a two step process, run through a hashing algorithm and re-running the hashing function; Weschler, column 16 lines 1-12).** Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to

implement the technique of Weschler within the system of Haverinen in order to create a secure data transfer through a re-authentication and key agreement process.

5. Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to CHHEAN THAO whose telephone number is (571)270-7497. The examiner can normally be reached on Monday-Friday 8:00 am-5:30pm; off every other Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nick Corsaro can be reached on 571-272-7876. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/CHHEAN THAO/
Examiner, Art Unit 2617

/NICK CORSARO/

Supervisory Patent Examiner, Art Unit 2617